Listing of Claims:

1-25. (Cancelled)

26. (New) A method for periodically renewing content protection implementations in devices, the method comprising:

on a first periodic basis, automatically pushing a new content protection implementation to a device that contains an existing content protection implementation;

wherein the existing content protection implementation comprises (a) existing software for presenting protected content and (b) an existing key to facilitate presentation of protected content; and

wherein the new content protection implementation comprises (a) new software to replace at least part of the existing software for presenting protected content and (b) a new key to supersede the existing key for facilitating presentation of protected content; and

on a second periodic basis, automatically pushing revocation data to the device, the revocation data to identify a revoked key, the revoked key comprising a key that has been superseded by the new key of the new content protection implementation;

wherein the revocation data to identify the revoked key is pushed to the device after a corresponding new content protection implementation has already been pushed to the device to equip the device with a replacement key for the revoked key; and

wherein the operation of pushing the new content protection implementation to the device comprises providing the new content protection implementation based on a predetermined time period, without regard to whether or not the existing key has been compromised.

27. (New) A method according to claim 26, further comprising:

waiting a selected amount of time after pushing the new content protection implementation to the device before pushing corresponding revocation data to the device.

28. (New) A method according to claim 26, wherein the first periodic basis and the second periodic basis have substantially the same period.

29. (New) A method according to claim 26, wherein the revocation data comprises two values that identify a range of more than two revoked keys.

30. (New) A method according to claim 26, wherein the revocation data is encrypted and can only be decrypted by the new key of the new content protection implementation.

31. (New) A method according to claim 26, wherein the device comprises an information handling device from the group consisting of:

a consumer electronics device for accessing protected content; and

a software-implemented player application for accessing protected content.

32. (New) A method according to claim 26, further comprising:

receiving the revocation data, at a device manufacturer, from a key generation facility; and

pushing the revocation data to the device from the device manufacturer.

33. (New) A method according to claim 26, wherein the operation of pushing the new content protection implementation to the device comprises:

storing the new content protection implementation in a storage medium to be used by the device.

34. (New) A method according to claim 33, wherein the operation of storing the new content protection implementation in the storage medium comprises storing the new content protection implementation in at least one medium from the group consisting of:

a blank storage medium; and

a pre-recorded storage medium.

35. (New) A method according to claim 26, further comprising:

receiving the revocation data, at a broadcaster, from a key generation facility; and

broadcasting, for reception by multiple devices, broadcast content that includes the revocation data.

36. (New) An apparatus, comprising:

a tangible, machine-accessible medium; and

instructions in the machine-accessible medium which, when executed by a processing system, cause the processing system to perform operations comprising:

on a periodic basis, automatically pushing a new content protection implementation to a device that contains an existing content protection implementation;

wherein the existing content protection implementation comprises (a) existing software for presenting protected content and (b) an existing key to facilitate presentation of protected content; and

wherein the new content protection implementation comprises (a) new software to replace at least part of the existing software for presenting protected content and (b) a new key to supersede the existing key for facilitating presentation of protected content; and

on a periodic basis, automatically pushing revocation data to the device, the revocation data to identify a revoked key, the revoked key comprising a key that has been superseded by the new key of the new content protection implementation;

wherein the revocation data to identify a revoked key is pushed to the device after a corresponding new content protection implementation has already been pushed to the device to equip the device with a replacement key for the revoked key; and

wherein the operation of pushing the new content protection implementation to the device comprises providing the new content protection implementation based on a predetermined time period, without regard to whether or not the existing key has been compromised.

37. (New) An apparatus according to claim 36, wherein the first periodic basis and the second periodic basis have substantially the same period.

38. (New) An apparatus according to claim 36, wherein the revocation data comprises two values that identify a range of more than two revoked keys.

39. (New) An apparatus according to claim 36, wherein the device comprises in information handling device from the group consisting of:

a consumer electronics device for accessing protected content; and
a software-implemented player application for accessing protected content.

40. (New) An apparatus according to claim 36, wherein the operations comprise:

receiving the revocation data from a key generation facility; and
pushing the received revocation data to the device.

41. (New) An apparatus according to claim 36, wherein the operation of pushing the new content protection implementation to the device comprises:

storing the new content protection implementation in a storage medium to be used by the device.

42. (New) An apparatus according to claim 41, wherein the storage medium comprises at least one medium from the group consisting of:

a blank storage medium; and

a pre-recorded storage medium.

43 (New) An apparatus according to claim 36, wherein the operation of pushing the revocation data to the device comprises:

including the revocation data in broadcast content transmitted by a broadcaster for reception by multiple devices.

44. (New) A device, comprising:

a processor;

a machine-accessible medium responsive to the processor;

an existing content protection implementation comprising (a) existing software for presenting protected content and (b) an existing key to facilitate presentation of protected content; and

instructions in the machine-accessible medium which, when executed by the device, enable to device to perform operations comprising:

receiving a new content protection implementation pushed to the device, the new content protection implementation comprising (a) new software to replace at least part of the existing software for presenting protected content and (b) a new key to supersede the existing key for facilitating presentation of protected content; and

receiving revocation data pushed to the device, the revocation data to identify a revoked key, the revoked key being a key that has been superseded by the new key from the new content protection implementation;

wherein the device receives the new content protection implementation with the new key before receiving the revocation data to revoke the existing key; and

wherein the operation of receiving the new content protection implementation comprises receiving the new content protection implementation based on a predetermined time period, without regard to whether or not the existing key has been compromised.

45. (New) A device according to claim 44, wherein the revocation data comprises two values that identify a range of more than two revoked keys.

46. (New) A device according to claim 44, wherein the device comprises in information handling device from the group consisting of:

a consumer electronics device for accessing protected content; and

a software-implemented player application for accessing protected content.

47. (New) A device according to claim 44, wherein the operation of receiving the new content protection implementation comprises receiving the new content protection implementation from a pre-recorded storage medium.

48. (New) A device according to claim 44, wherein the operation of receiving the revocation data comprises:

receiving the revocation data from broadcast content transmitted by a broadcaster for reception by multiple devices.

49. (New) A device according to claim 44, wherein the operations further comprise:

after receiving the revocation data, processing the revocation data prior to allowing access to protected content.